
ACP

Hannes Lagler-Gruener

Cloud Solutions Architect, ACP

P-CSA, Azure MCSE, AWS Cloud Practitioner

Blog https://cloudblogger.at

LinkedIn https://www.linkedin.com/in/hannesl1

Twitter @HannesLagler

IT for innovators.

Agenda

- Azure governance scaffold
- Azure hierarchy and management groups
- Resource groups and tagging
- Naming standards
- Azure policy and initiatives
- Identity and access management
- Security
- Cost management

IT for innovators.

The future is already here it's just not very evenly distributed.

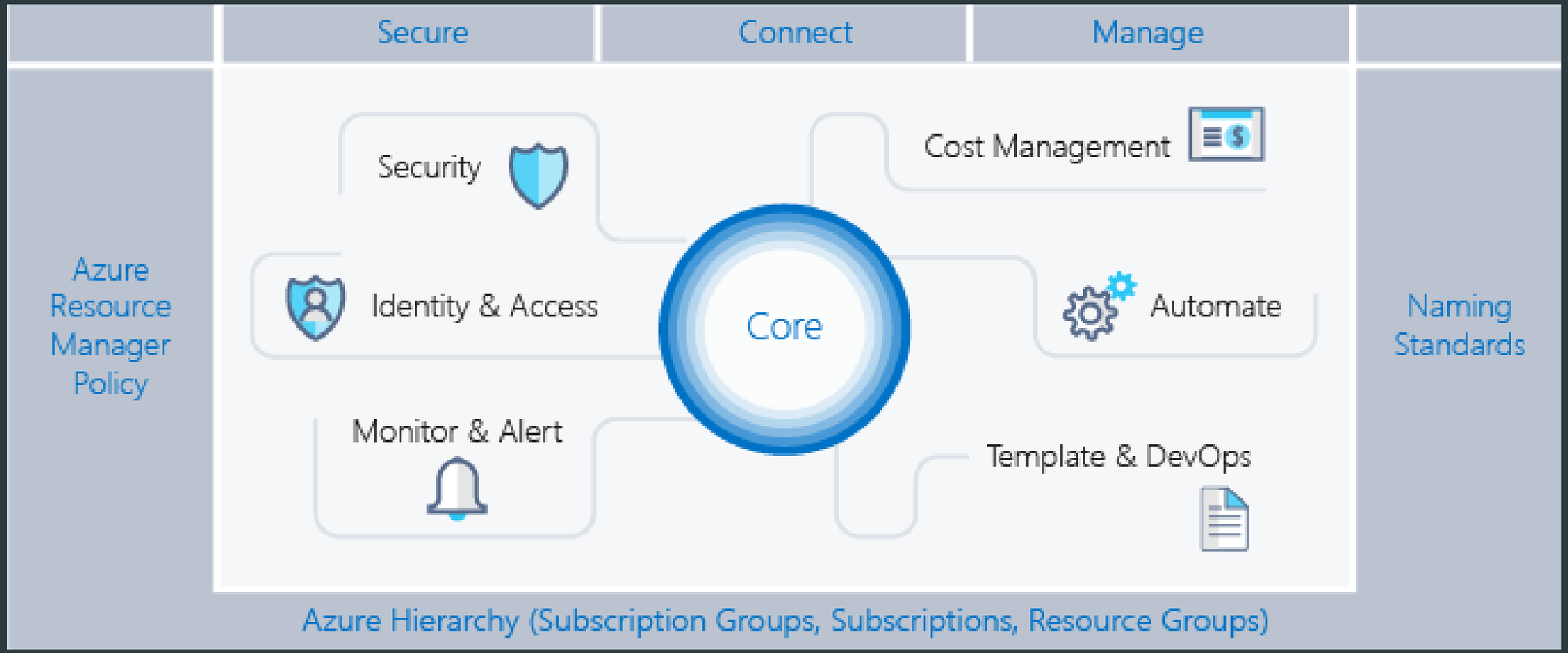
William Gibson

IT for innovators.

Azure Governance Scaffold

IT for innovators.

Azure Governance Scaffold



IT for innovators.

Azure Hierarchy and management groups

IT for innovators.

Depends on billing method

Azure Hierarchy

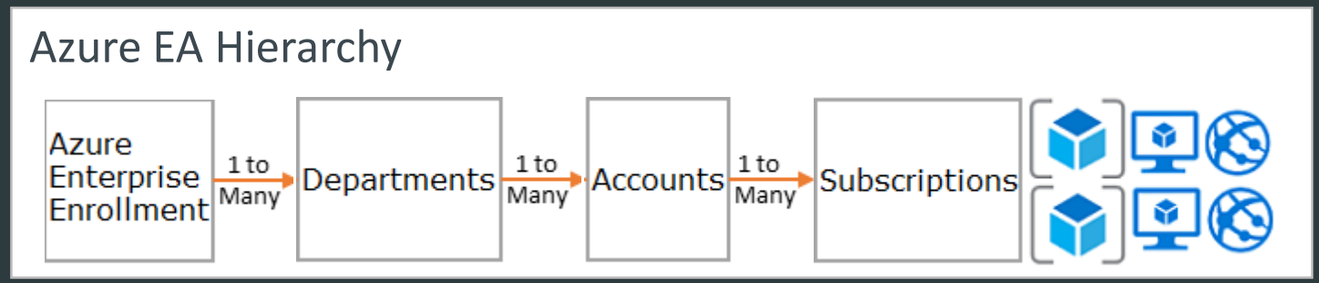
- Different billing methods
  - Microsoft direct
  - Microsoft Enterprise Agreement
  - Partner CSP

IT for innovators.

Azure Enterprise Agreement

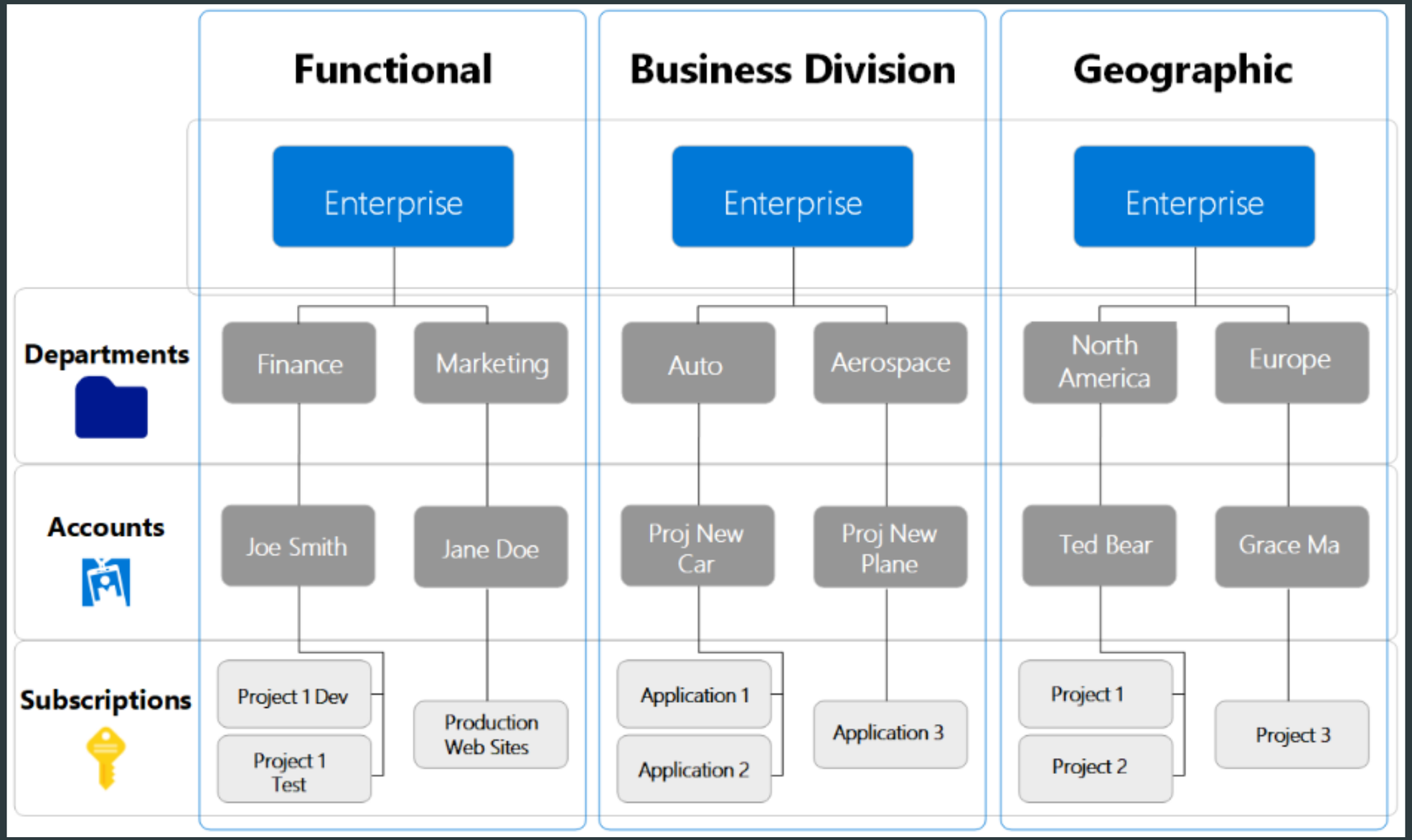
Azure EA Hierarchy

- Enterprise administrator
  - Highest level of access
- Department administrator
  - Manage departments
  - Create new account owners
  - View usage details
  - View costs
- Account owner
  - Create and manage subscriptions
  - Manage service administrators
  - View usage for subscriptions
- Service administrator
  - Manage services in the Azure portal



IT for innovators.

Azure Enterprise Agreement



IT for innovators.

To complex and not flexible enough!
The new way:

IT for innovators.

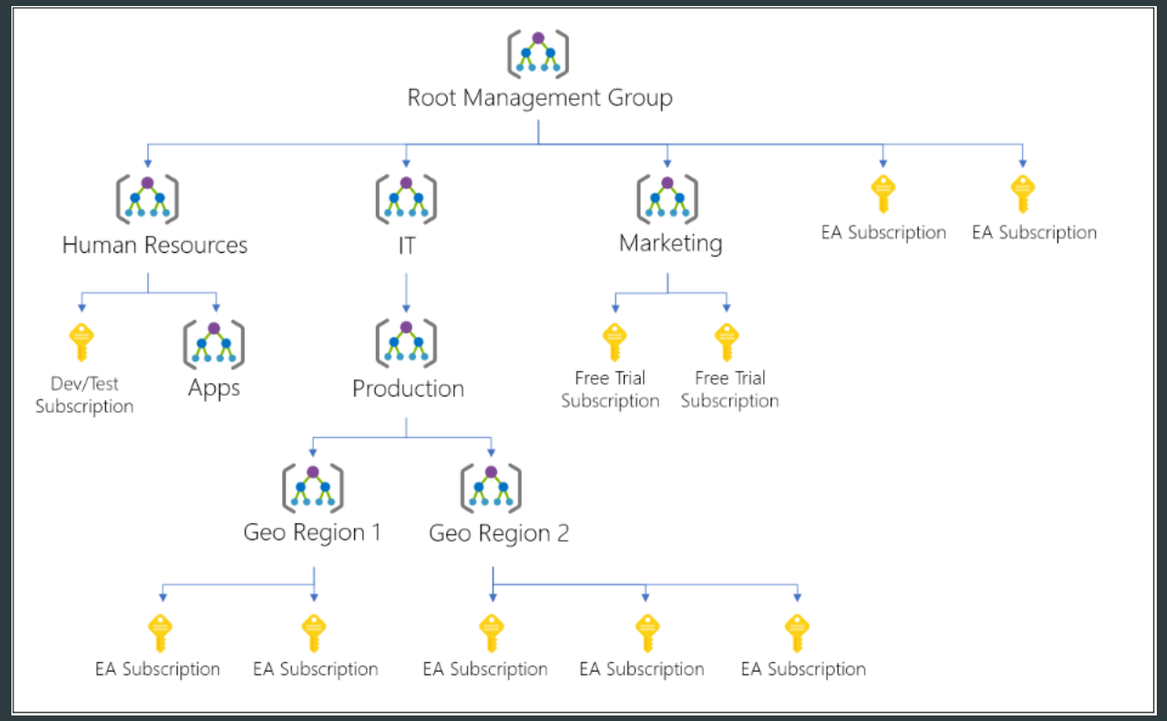
Azure Management Groups

IT for innovators.

Azure Management Group

Important facts:

- 10.000 Management groups/single directory
- Max. six levels of deep
- Each management and subscription support only on parent
- Each management group can have many children



Best practice:

- Keep it simple
- Use a guide for management ID

IT for innovators.

Demo

IT for innovators.

- Azure Management Groups

Agenda

- ✓ Azure governance scaffold
- ✓ Azure hierarchy and management groups
- ➢ Resource groups and tagging
- ➢ Naming standards
- ➢ Azure policy and initiatives
- ➢ Identity and access management
- ➢ Security
- ➢ Cost management

IT for innovators.

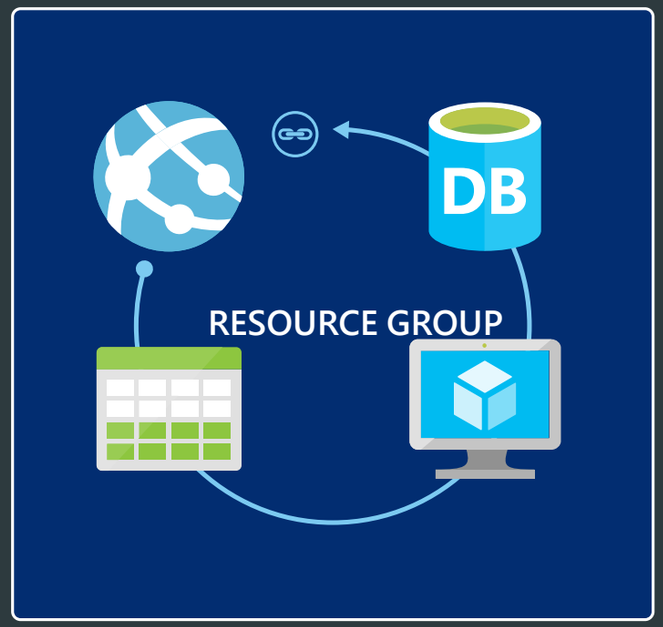
Resource groups and tagging

IT for innovators.

Azure resource group

"Traditional IT" workloads to "Agile IT" workloads

- Traditional IT: workloads are most commonly grouped by items within the same lifecycle
- Agile IT: reflect the layers of deployment (web tier or app tier)



Important facts:

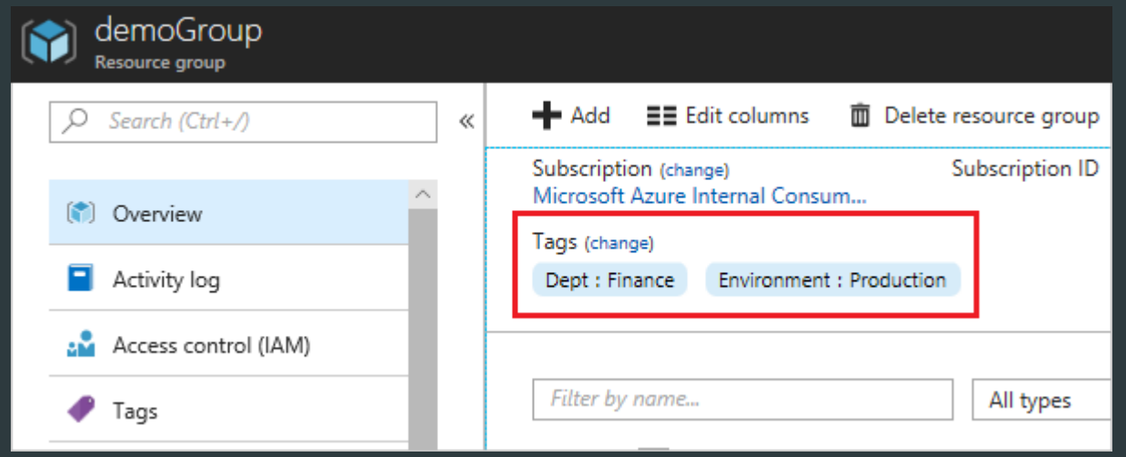
- Only one resource group per resource
- Resource groups aren‘t region bound
- Resource group nesting isn‘t allowed
- Create resource groups need higher permissions

IT for innovators.

Azure resource tagging

Important facts:

- Use tags to organize your Azure resources
- Define a naming standard for tags
- Plan for management of your tags carefully
- Tags can contain personal information (GDBR)
- Use tags for your billing and management
- Tags are often used as part of automation



Samples

- Environment
- Role
- Department
- CostCenter

IT for innovators.

ACP

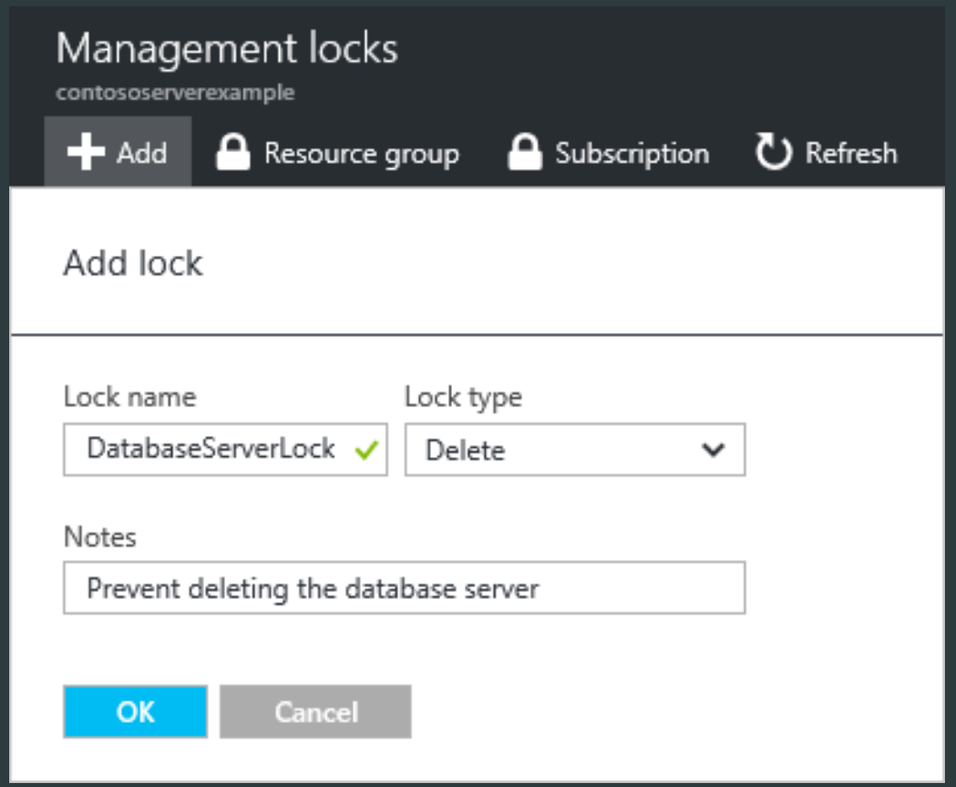
Resource Lock

IT for innovators.

Azure resource lock

Important facts:

- Protect resource
  - Delete Lock
  - Read-Only Lock
- Assign to
  - Subscription
  - Resource Groups
  - Resources



IT for innovators.

Naming Standards

IT for innovators.

Azure naming standard

Important facts:

- High important task
- It‘s a dynamic task
- Required task for automation
- Service rename isn‘t possible!

```
<Company> <Department (optional)> <Product Line (optional)> <Environment>
```

IT for innovators.

Demo

- Resource groups
  - Resource lock
- Resource tagging

IT for innovators.

Agenda

- ✓ Azure governance scaffold
- ✓ Azure hierarchy and management groups
- ✓ Resource groups and tagging
- ✓ Naming standards
- ➢ Azure policy and initiatives
- ➢ Identity and access management
- ➢ Security
- ➢ Cost management

IT for innovators.

Azure policy and initiatives

Azure policy:

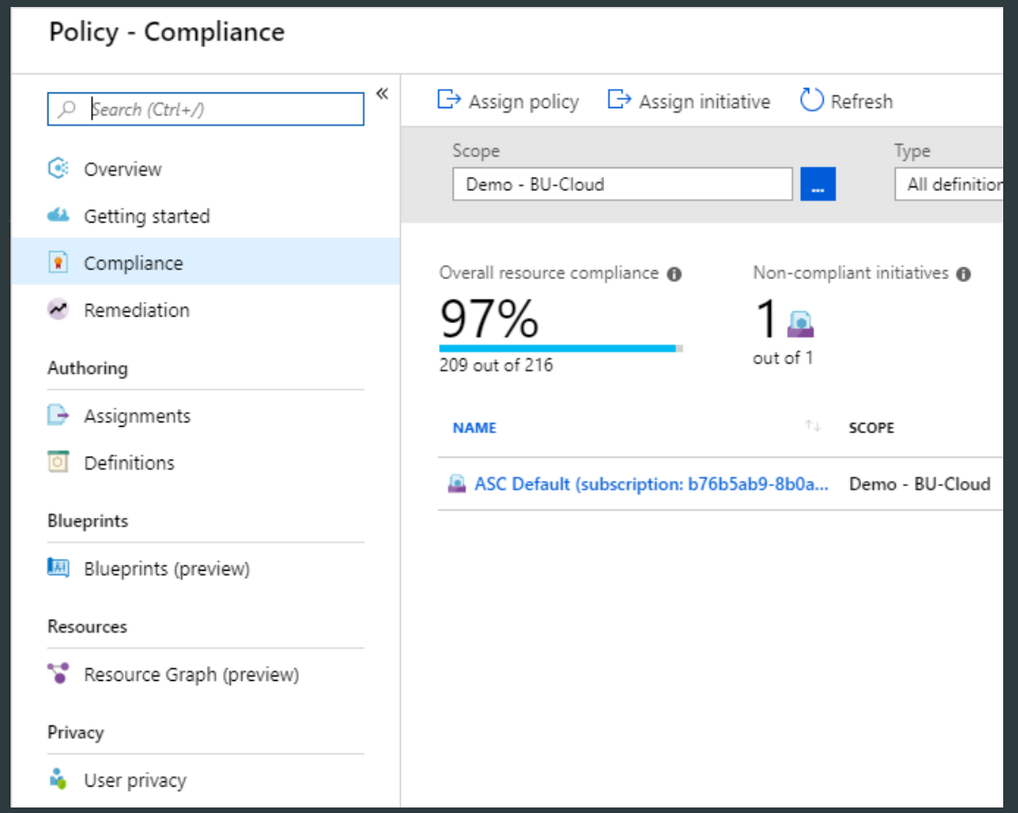
- Policies allow companies to provide controls
- Two policy types:
  - Audit
  - Enforce

Typical policies:

- Allowed Storage Account SKUs
- Allowed Resource Type
- Allowed Locations
- Allowed Virtual Machine SKUs

Azure initiative:

- A collection of Azure policies



IT for innovators.

Identity and access management

IT for innovators.

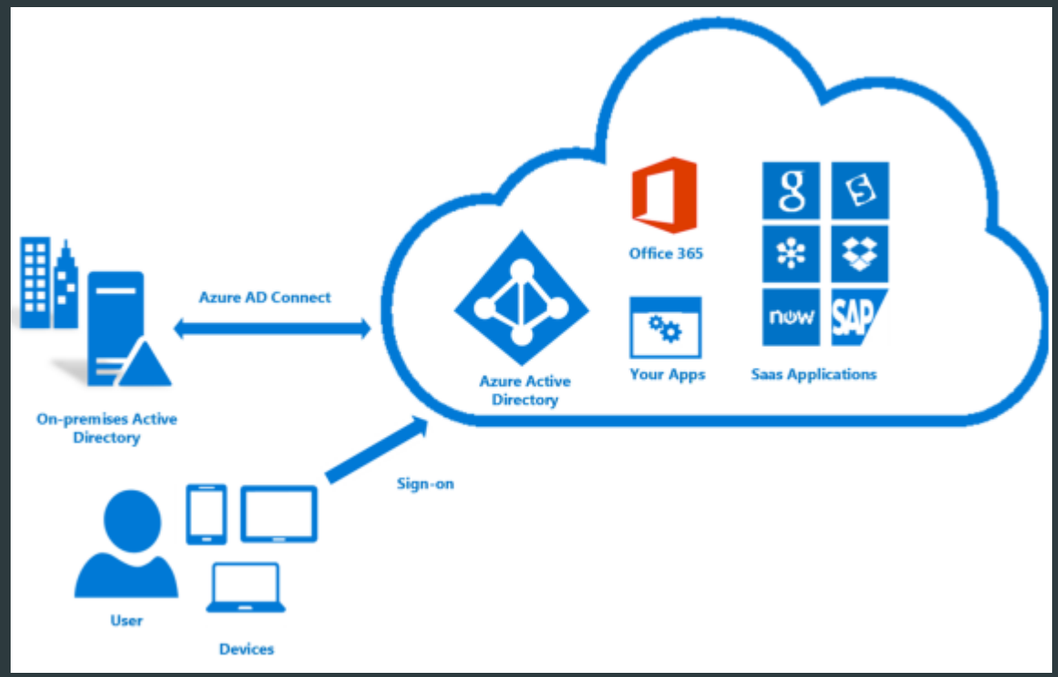
Azure identity

Important facts:

- Managed or federation?

Federation:

- Implement AD-Connect
- PW Hash sync, ADFS or PTA?
- Sync user and groups to Azure AD
- Azure AD hardening!



IT for innovators.

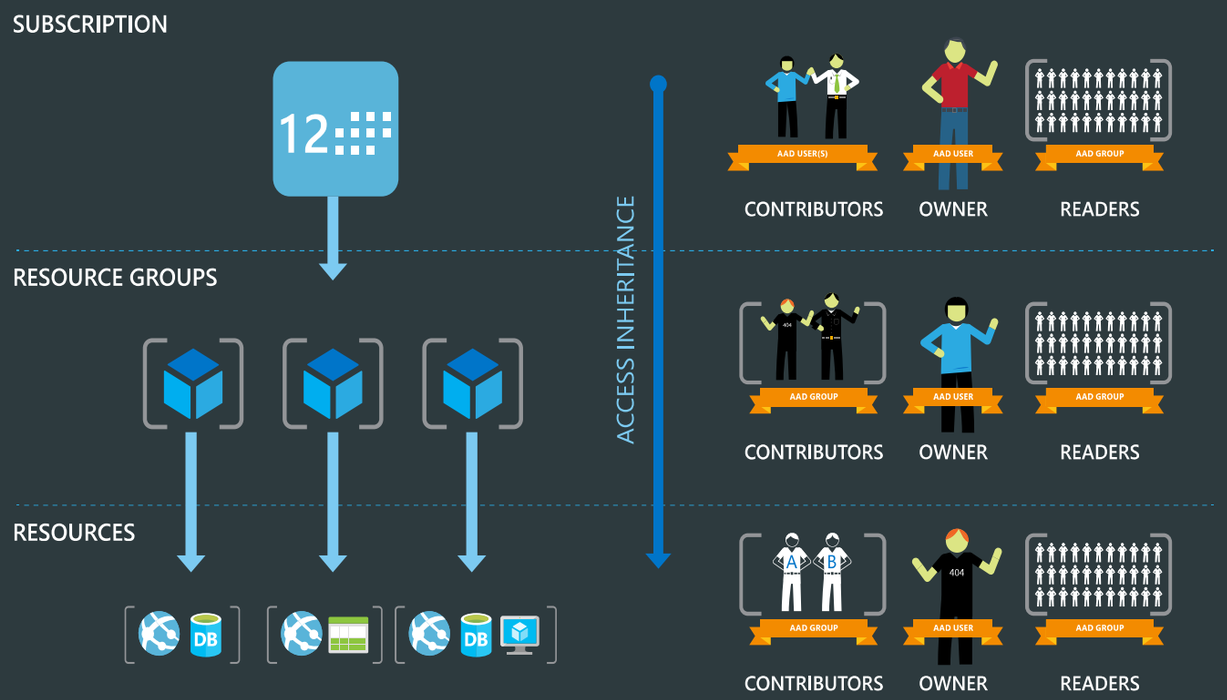
Azure access management

Important facts:

- Least privilege!
  - Azure AD PIM (depends on license)
- Audit a monitor azure access
- Control access
  - Azure portal (for managed domain)
  - On-Prem (for federated domain)

RBAC:

- Keep it simple!
  - Azure AD
  - Office 365
  - Azure Subscription



IT for innovators.

Demo

- Azure policy/initiative
- Azure access management
  - Azure RBAC

IT for innovators.

Agenda

- ✓ Azure governance scaffold
- ✓ Azure hierarchy and management groups
- ✓ Resource groups and tagging
- ✓ Naming standards
- ✓ Azure policy and initiatives
- ✓ Identity and access management
- ➢ Security
- ➢ Cost management

IT for innovators.

Azure Security

IT for innovators.

Azure Security

Quelle: https://servicetrust.microsoft.com/Documents/ComplianceReports

IT for innovators.

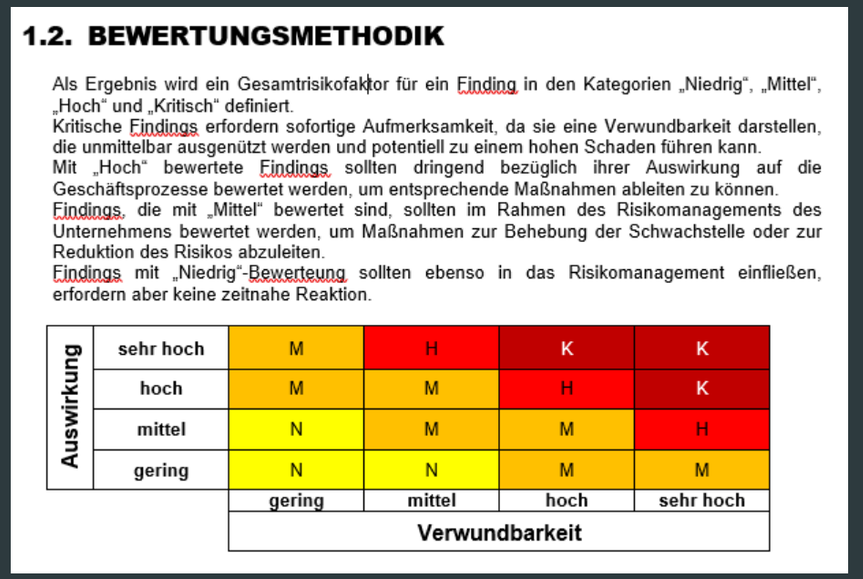
Azure Security Continue

IT for innovators.

ACP Azure AD hardening

Azure
Security
Continue

- Segregation of duty
- Microsoft best practice
- ACP best practice
- Get a result report



1.2. BEWERTUNGSMETHODIK

Als Ergebnis wird ein Gesamtrisikofaktor für ein Finding in den Kategorien „Niedrig“, „Mittel“, „Hoch“ und „Kritisch“ definiert.
Kritische Findings erfordern sofortige Aufmerksamkeit, da sie eine Verwundbarkeit darstellen, die unmittelbar ausgenützt werden und potentiell zu einem hohen Schaden führen kann.
Mit „Hoch“ bewertete Findings sollten dringend bezüglich ihrer Auswirkung auf die Geschäftsprozesse bewertet werden, um entsprechende Maßnahmen ableiten zu können.
Findings, die mit „Mittel“ bewertet sind, sollten im Rahmen des Risikomanagements des Unternehmens bewertet werden, um Maßnahmen zur Behebung der Schwachstelle oder zur Reduktion des Risikos abzuleiten.
Findings mit „Niedrig“-Bewerteung sollten ebenso in das Risikomanagement einfließen, erfordern aber keine zeitnahe Reaktion.

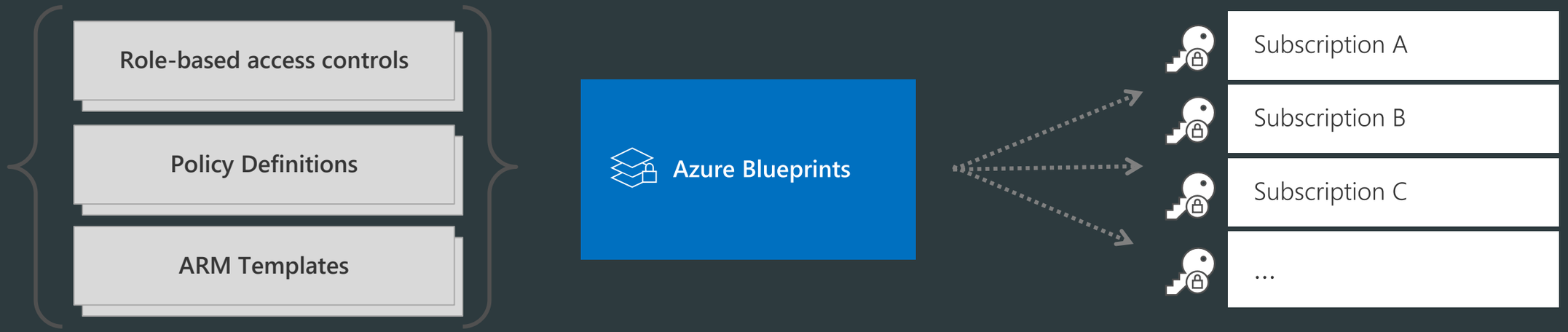
Auswirkung					
	sehr hoch	M	H	K	K
	hoch	M	M	H	K
	mittel	N	M	M	H
	gering	N	N	M	M
		gering	mittel	hoch	sehr hoch
		Verwundbarkeit			

IT for innovators.

Azure access management

Declarative way to orchestrate the deployment of various resource templates and other artifacts such as:

- Role Assignments
- Policy Assignments
- Azure Resource Manager templates
- Resource Groups



IT for innovators.

Cost management

IT for innovators.

Azure access management

Azure portal capabilities:

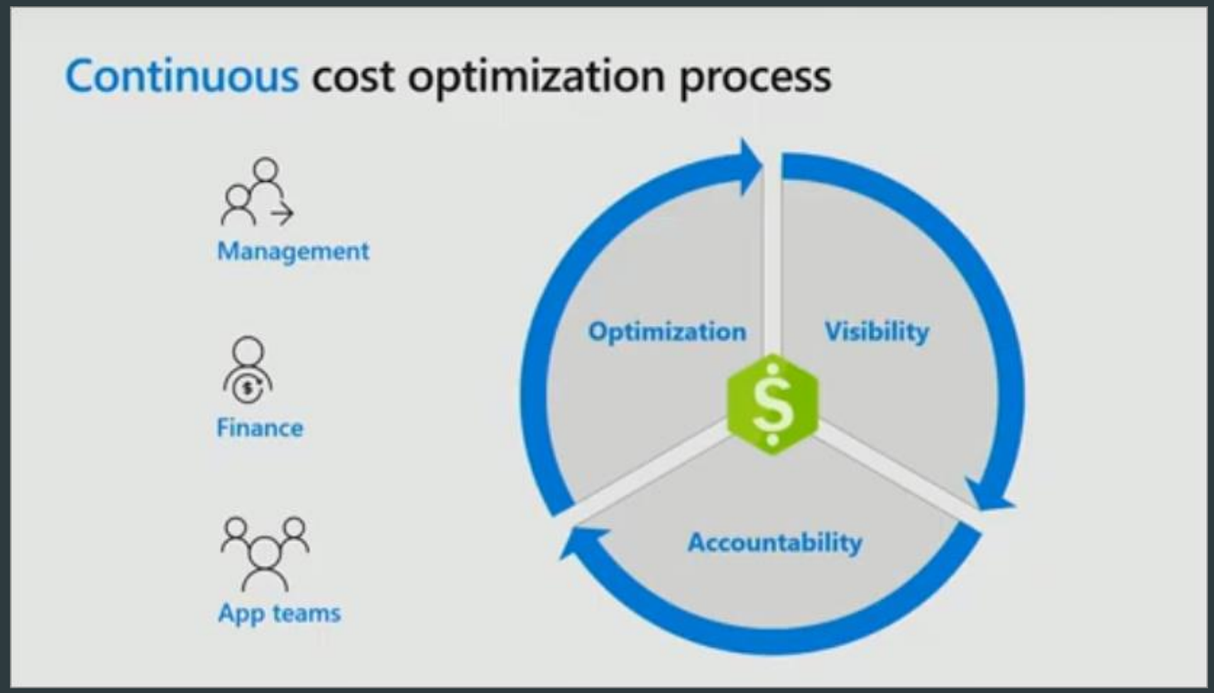
- Subscription resource cost
- Azure Cost Management
- Azure budgets and action groups
- Azure Advisor

External cost management tools

- Power BI Azure Consumption Insights
- Consumption API

Best practice:

- Actively monitor costs
- Use Reserved VM Instances
- Use automation effectively
- Use resource tags for visibility



IT for innovators.

Demo

- Azure security
  - RBAC, Security Center, BluePrint
- Azure Cost management
  - Cost analysis
  - Azure Budget
  - Azure Advisor

IT for innovators.

Agenda

- ✓ Azure governance scaffold
- ✓ Azure hierarchy and management groups
- ✓ Resource groups and tagging
- ✓ Naming standards
- ✓ Azure policy and initiatives
- ✓ Identity and access management
- ✓ Security
- ✓ Cost management

IT for innovators.

Thank you

Hannes Lagler-Gruener
Cloud Solutions Architect, ACP
P-CSA, Azure MCSE, AWS Cloud Practitioner

Blog http://cloudblogger.at
LinkedIn https://www.linkedin.com/in/hannesl1
Twitter @HannesLagler

IT for innovators.